

**PKI DIGITAL SIGNATURE
CERTIFICATE POLICY**

version as of September 1, 2001
the current version may be found at
<http://www.sos.state.az.us/pa/default.htm>

**State of Arizona
Policy Authority
Office of the Secretary of State**

**ARIZONA ELECTRONIC SIGNATURE INFRASTRUCTURE (AESI)
Public Key Infrastructure (PKI)
VERSION 2.0
September 2001**

TABLE OF CONTENTS

1	Introduction.....	1
2	Policy Specification.....	1
2.1	Overview	1
2.2	Policy overview.....	2
2.3	Identification alphanumeric OID	3
2.4	Community and applicability.....	3
2.4.1	Certification Authorities (CAs).....	4
2.4.2	CAs Authorized to Issue Certificates under this Policy.....	4
2.4.3	Registration Authorities and Certificate Manufacturing Authorities.....	5
2.4.4	Local Registration Authorities (LRAs).....	5
2.4.5	Repositories.....	5
2.4.6	Subscribers.....	5
2.4.7	Relying parties	5
2.4.8	Policy applicability	6
2.4.9	Approved and prohibited applications	6
2.4.9.1	Approved Applications	6
2.4.9.2	Prohibited Applications	6
2.4.10	Contact details	6
2.4.10.1	Policy Authority contact person:.....	6
2.4.10.2	Contact person determining CPS suitability for this Policy:.....	6
3	General Provisions	7
3.1	Obligations	7
3.1.1	CA obligations	7
3.1.1.1	Representations By CA.....	7
3.1.1.2	Time between certificate request and issuance.....	7
3.1.2	Registration Authorities (RA) and Certificate Manufacturing Authorities (CMA) Obligations	7
3.1.3	Repository Obligations	8
3.1.4	LRA obligations (LRA duties).....	8
3.1.5	Subscriber Obligations	8
3.1.6	Relying Party Obligations	9
3.1.7	Policy Authority Obligations	9
3.2	Requirements	9
3.2.1	Financial Responsibility.....	9
3.2.1.1	Surety Bond	9
3.2.1.2	Insurance	10
3.2.1.3	Consequences of failure to meet Financial Responsibilities	10
3.3	Disclaimers of warranties and obligations	10
3.4	Liability.....	10
3.5	Interpretation & Enforcement	11
3.5.1	Governing Law	11
3.5.2	Severability, survival, merger, notice	11
3.5.3	Dispute Resolution Procedures	11
3.6	Fees	11
3.7	Publication & Repositories	11
3.7.1	Publication Of CA Information	11
3.7.2	Frequency of Publication.....	12

Draft

3.7.3	Access Controls	12
3.8	Compliance Audit	12
3.9	Confidentiality Policy	12
3.10	Intellectual property rights.....	12
4	Identification And Authentication.....	12
4.1	Initial Registration.....	12
4.1.1	Types of Names	13
4.1.2	Name Meanings	13
4.1.3	Rules For Interpreting Various Name Forms.....	13
4.1.4	Name Uniqueness	13
4.1.5	Verification of Key Pair	13
4.1.6	Authentication of Organization.....	13
4.1.7	Authentication of Individual -- No Affiliation.....	14
4.1.7.1	Identification.....	14
4.1.7.2	Investigation And Confirmation.....	14
4.1.7.3	Personal Presence	14
4.1.8	Authentication of Individual – Affiliated Certificate.....	14
4.1.8.1	Identification.....	14
4.1.8.2	Authentication Confirmation Procedure	15
4.1.8.3	Personal Presence	15
4.1.8.4	Duties of Responsible Individuals	15
4.1.9	Authentication of devices or applications	15
4.2	Renewal Applications (Routine Rekey)	15
4.3	Rekey After Revocation.....	15
4.4	Satisfactory Evidence of Identity.....	16
5	Operational Requirements	20
5.1	Certificate Application.....	20
5.1.1	Application for a cross-certificate.....	21
5.2	Certificate Issuance	21
5.3	Certificate Acceptance	21
5.4	Certificate Revocation.....	21
5.4.1	Circumstances For Revocation	21
5.4.1.1	Permissive Revocation.....	21
5.4.1.2	Required Revocation	22
5.4.2	Procedure For Revocation Request.....	22
5.4.2.1	Repository/CRL Update	23
5.4.3	Revocation Request Grace Period.....	23
5.4.4	Certificate Suspension.....	23
5.4.5	CRL Issuance Frequency.....	23
5.4.6	CRL checking requirements.....	23
5.4.7	On-Line Revocation/Status Checking Availability	23
5.4.8	Special requirements rekey compromise	23
5.5	Computer Security Audit Procedures	24
5.6	Records Archival.....	24
5.6.1	Types Of Records Archived.....	24
5.6.2	Retention Period For Archive	24
5.6.3	Protection Of Archive	24
5.6.4	Archive Backup Procedures.....	24
5.6.5	Archive Collection System (Internal Or External)	24
5.6.6	Procedures To Obtain And Verify Archive Information.....	24

Draft

5.7	Key Changelog	24
5.8	Compromise And Disaster Recovery	25
5.8.1	Disaster Recovery Plan	25
5.8.2	Key Compromise Plan	25
5.9	CA Termination	25
6	Physical, Procedural And Personnel Security	25
6.1	Physical Controls	25
6.1.1	Physical Security -- Access Controls	25
6.2	Procedural Controls	25
6.2.1	Trusted Roles	26
6.2.2	Multiple Roles (Number Of Persons Required Per Task)	26
6.3	Personal Security Controls	26
6.3.1	Background And Qualifications	26
6.3.2	Background Investigation	26
6.3.3	Training Requirements	26
6.3.4	Documentation Supplied To Personnel	26
7	Technical Security Controls	26
7.1	Key Pair Generation And Installation	26
7.1.1	Key Pair Generation	26
7.1.2	Private Key Delivery To Entity	27
7.1.3	Subscriber Public Key Delivery To CA	27
7.1.4	CA Public Key Delivery To Users	27
7.1.5	Key Sizes	27
7.2	CA Private Key Protection	27
7.2.1	Standards For Cryptographic Module	27
7.2.2	Private Key (N-M) Multi-Person Control	27
7.2.3	Private Key Escrow	27
7.2.4	Private Key Backup	27
7.2.5	Private Key Archival	27
7.2.6	Private Key Entry Into Cryptographic Module	27
7.2.7	Method Of Activating Private Key	28
7.2.8	Method Of Deactivating Private Key	28
7.2.9	Method Of Destroying Private Key	28
7.3	Other Aspects Of Key Pair Management	28
7.3.1	Public Key Archival	28
7.3.2	Key Replacement	28
7.3.3	Restrictions On CA's Private Key Use	28
7.4	Activation Data	28
7.5	Computer Security Controls	28
8	Certificate And CRL Profiles	29
8.1	Certificate Profile	29
8.1.1	Certificate extensions	29
8.2	CRL Profile	29
8.2.1	Version number	29
8.2.2	CRL and CRL entry extensions	29
9	Policy Administration	29
9.1	Policy Change Procedures	29
9.1.1	List Of Items	30
9.1.2	Comment Period	30
9.2	Publication & Notification Procedures	30

Draft

9.2.1.1	Notification mechanism.....	30
9.2.1.2	Mechanism to handle comments	30
9.2.2	Items whose change requires a new policy.....	30
9.3	CPS approval procedures.....	30

1 **Introduction**

This Certificate Policy (Policy) defines Arizona's Digital Signature Certificate Policy – Basic Assurance Level. This Policy is for use in the Public Key Infrastructure (PKI)¹ portion of the State of Arizona's Electronic Signature Infrastructure (AESI)² as defined and managed by Arizona's Policy Authority (PA). The Policy Specification portion of this document is modeled after and complies with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework.

This document uses several technical concepts associated with PKI technology. To become familiar with the terminology used, we strongly recommend that you read the Electronic and Digital Signature Definitions and Acronyms document before reading this one and then refer to it as needed while reading this.

The security mechanisms provided by the AESI are not intended to be used alone for the protection of classified or sensitive information.

2 **Policy Specification**

2.1 **Overview**

The certificate policy defined in this document is intended for use by agencies and departments of the State of Arizona and anyone having digital signature use with them. Users of this document are to consult the issuing Certification Authority (CA) to obtain further details of the specific implementation of this Certificate Policy (CP).

Parties that find the Certificate Policies issued by the Policy Authority do not exactly meet their needs should accept and use the closest *less* restrictive CP and create a binding agreement between them that adds whatever additional conditions they require. They may not reduce or otherwise undermine the terms and conditions of the accepted CP. Relying Parties rely on the stated CP being fully enforceable.

The digital signature policies within this CP are for the management and use of Certificates used for verification, authentication, integrity and key agreement mechanisms. For instance, the Certificates issued under this policy could be used for verifying the identity of electronic mail correspondents or for remote access to a computer system, verifying the identity of citizens or other legal entities, or protecting the integrity of software and documents.

The term “assurance” is not intended to convey any representation or warranty as to 100% availability of CA services offered within the AESI. Such availability may be affected by system maintenance, system repair or factors outside the control of the CA. The State of

¹ “A collection of certificates, with their issuing CA's, subjects, relying parties, RA's, and repositories, is referred to as a Public Key Infrastructure, or PKI.” from the IETF draft *Internet X.509 Public Key Infrastructure PKIX Roadmap* (draft-ietf-pkix-roadmap-02.txt)

² taking liberties with IETF's conception of PKI, AESI is Arizona's collections (note plural) of electronic signing mechanisms and the entities and tools that support and provide the means to validly use these mechanisms as signatures.

Arizona has an active goal of "5 9's"³ but does not represent or warrant 100% availability offered within the AESI.

Issuance of a Certificate under any of these policies does not imply that the Subscriber has any authority to conduct business transactions on behalf of an organization.

The CA will be governed by the laws of the State of Arizona and any applicable Federal and local law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

The State of Arizona will not enter into a cross certification agreement with a Certification Authority not approved by the Policy Authority.

2.2 Policy overview

The Policy Object Identifier Designation for this Policy is registered under the Policy Authority arc { joint-iso-ccitt (2) country (16) us (840) state (3) AZ (04) EB (01) Secretary of State (002) DO (02) Policy Authority (999) } as OO (00) id-AESIpki-certpcy-sign-2 (002). This policy has been designed to be used in certain situations and identifies specific roles to implement them. Certificate Authorities (CA), Local Registration Authorities (LRAs), Certificate Manufacturing Authority (CMA), Subscribers and Relying Parties all have specific obligations which are outlined in this policy.

A CA may issue cross-certificates at this level of assurance and is obliged to inform Subscribers which uses are intended within AESI. Any cross-certification to external organizations will only be done by and through the AESI's topCA.

A CA must ensure that it associates itself with, and uses, one Certificate and one CRL repository for this type of certificate. Certificates must be made available to Subscribers.

The appropriate use of this assurance level's certificates and keys is for signing documents that, if compromised, could cause minimal injury to the interests of the State of Arizona.

The State of Arizona disclaims all liability for any use of this type of certificate other than uses permitted within this document. The State of Arizona limits its liability for permitted uses to \$5,000 per instance of use.

Any disputes concerning key or certificate management under this policy are to be resolved by the Parties concerned using an appropriate dispute settlement mechanism (i.e. through negotiation, mediation or arbitration).

Certificates may be issued under this policy following authentication of a Subscriber's identity.

Identification and authentication will be in the manner set out in this policy.

A CA will revoke certificates in the circumstances enumerated in this policy.

³ 5 9's (five nines) refers to a goal of 99.999% uptime, that is, the system is accessible 99.999% of the calendar year.

A CA is required to maintain records or information logs in the manner described in this policy.

A CA should ensure that critical CA functions are performed by at least two individuals.

Digital signature keys must not be backed-up or otherwise stored. Keys may have a validity period as indicated in this policy.

This CP does not allow the ability to recover any private key. The private key is in the sole possession of the subscriber. Applications that require recoverable encrypted messaging will employ a CP defining confidentiality with key recovery *for encryption only*. Such applications may also use this CP, but only for a separate *electronic signature* and as long as there is no mingling of the two types of Certificates in a repository. Certificates based on this Certificate Policy rely on the Subscriber's sole possession to assert the right of Non-Repudiation and must not be mingled with any Certificates that allow recovery and thereby break the criteria of sole possession.

No personal information collected by a CA may be disclosed without the Subscriber's consent unless required by law. The CA may not sell any information under any circumstance that is not specifically allowed by this CP.

CA activities are subject to inspection by the PA and agents of the PA.

2.3 Identification

2.3.1 alphanumeric OID

id-AESIpki-certpcy-digitalSignature-basicAssurance ::= { id-AESIpki-certpcy-sign-2 }

2.3.2 Certificate Types

The following certificate types and OIDs will be recognized for use within the ESI established by this Certificate Policy (OID 2.16.840.3.04.01.002.02.999.00.002). The certificate types listed below — Basic, Medium and High — vary depending on the method of identifying the Signer, the method for linking the Signer to the Certificate and the processes for assuring the Integrity of the Record. The ESI electronic signature level (Basic, Medium, High) is determined from the matrix of trust levels in section 2. The Certificate assigned should support the highest trust level required among the categories: Signer Identification, Signer Linkage to Signature, and Signature Linkage to the Integrity of the Record. Each level of Certificate subsumes the level(s) below it. All Certificates issued under this Certificate Policy will contain the OID listed below in the Certificate Policies field of the Certificate:

- Basic Trust Signing Certificate OID is: 2.16.840.3.04.01.002.02.999.00.002.01.01
- Medium Trust Signing Certificate OID is: 2.16.840.3.04.01.002.02.999.00.002.01.02
- High Trust Signing Certificate OID is: 2.16.840.3.04.01.002.02.999.00.002.01.03

2.4 Community and applicability

The State of Arizona's Electronic Signature Infrastructure (AESI), and consequently, its Public Key Infrastructure (PKI), is managed by the Office of the Secretary of State serving as the Policy Authority (PA) in accordance with appropriate Statute and Administrative Rules.

This Electronic Signature Infrastructure (ESI) is designed to enable the use of electronic signatures as the equivalent of handwritten signatures. This requires a similar range of protections of the authenticity and verification as a handwritten signature on a physical document. It also requires, given its nature, additional protections that the signer cannot repudiate their signing later. This Policy describes a bounded public key infrastructure within AESI.

2.4.1 Certification Authorities (CAs)

This Policy is binding on each Approved CA that issues certificates that identify this Policy, and governs the CA's performance with respect to all certificates the CA issues that reference this Policy. Specific practices and procedures by which the CA implements the requirements of this Policy shall be set forth by the CA in a certification practice statement ("CPS") or other publicly available document.

A CA operating under this policy is responsible for the creation and signing of:

- Certificates binding Subscribers, PKI personnel and (where permitted) other CAs with their signature verification keys;
- promulgating certificate status through CRLs; and
- ensuring adherence to this Certificate Policy.

All Subscribers shall use CAs approved by the Policy Authority. Should a state Agency use a contractor to provide CA services, the Agency will remain responsible and accountable for the operation of its CA.

The topCA of *AESI PKI* is the CA governed directly by the PA (or designated as such by the PA). All other CAs are required to supply all repository and CRL information to it while they operate independent of it. AESI PKI Agency Level CAs will cross-certify only with the topCA. A cross-certification must be in accordance with the selected Certificate Policy and any additional requirements determined by the PA.

All cross-certification between AESI CAs and non-AESI CAs will be done through the topCA pursuant to instructions from the PA. Any agreements made with other CAs must be documented and have applicable disclaimers made available to Subscribers.

A CA may issue cross-certificates to other AESI CAs where expressly authorized by the PA.

2.4.2 CAs Authorized to Issue Certificates under this Policy

A CA may issue certificates that identify this Policy only if such CA first qualifies as an Approved CA by:

- a) entering into an agreement with the Policy Authority, for the benefit of all Qualified Relying Parties, to be bound by, and comply with, the undertakings and representations of this Policy, with respect to the class of certificates that are issued with reference to this Policy, and
- b) being approved by the Policy Authority, following successful completion of the compliance audit specified herein, a review of its CPS, and satisfaction of the insurance requirements specified herein.

2.4.3 Registration Authorities and Certificate Manufacturing Authorities

The role and functions of the Registration Authority (RA) shall be performed by each Approved CA. An Approved CA may subcontract Registration Authority functions to third party RAs who agree to be bound by this Policy, but the Approved CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its AESI Contract.

The role and functions of the Certificate Manufacturing Authority (CMA) shall be performed by each Approved CA. An Approved CA may subcontract CMA functions to third party CMAs who agree to be bound by this Policy, but the Approved CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its AESI Contract.

2.4.4 Local Registration Authorities (LRAs)

An LRA operating under this certificate policy is responsible for all duties assigned to it by the CA.

An LRA may perform duties on behalf of more than one CA, providing that in doing so it satisfies all the requirements of this CP.

2.4.5 Repositories

The Repository's role and functions shall be performed by each Approved CA. An Approved CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this Policy, provided that such subcontractor is approved in advance by PA, but the Approved CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its PA Contract.

2.4.6 Subscribers

A CA may issue Certificates that reference this Policy to the following classes of subscribers:

- individuals (unaffiliated)
- individuals associated with a sponsor recognized by the CA ("affiliated individuals"), provided the sponsor is the Subscriber of a valid Certificate issued by the CA in accordance with this Policy.
- organizations that qualify as legal entities provided that responsibility and accountability is attributable to an designated living agent for the organization.
- government agencies provided that responsibility and accountability is attributable to an designated living agent for the agency.

Subscribers may also be issued Certificates for assignment to devices or applications provided that responsibility and accountability is attributable to the subscriber.

2.4.7 Relying parties

This Policy is intended for the benefit of the following persons who may rely on Certificates issued to others that reference this Policy (Qualified Relying Parties):

- State government agencies that specify this Policy by regulation
- Federal and other government agencies that specify this Policy by regulation

- Businesses that agree to accept AESI Certificates and agree to be bound by the terms of this Policy regarding those Certificates.
- Individuals that agree to accept AESI Certificates and agree to be bound by the terms of this Policy regarding those Certificates.

2.4.8 Policy applicability

This Certificate Policy is suitable for the integrity and authentication of business transactions within the originator's approval limits and such that the falsification of the transaction would cause only minor financial loss or require only administrative action for correction.

2.4.9 Approved and prohibited applications

Certificates that reference this Policy are intended to support verification of digital signatures in applications where the identity of communicating parties needs to be authenticated, where a message or file needs to be bound to the identity of its originator by a signature, and/or where the integrity of the file or message has to be assured.

2.4.9.1 Approved Applications

Certificates that reference this Certificate Policy may be used for any purpose authorized by regulations adopted by Qualified Relying Parties unless they diminish the provisions of the Certificate Policy or are specifically prohibited by agreements among the ESI Signers and Relying Parties.

2.4.9.2 Prohibited Applications

Certificates that reference this Policy may not be used for any application requiring fail-safe performance such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or environmental damage.

Certificates that reference this Policy should not be used for transactions where the per use value exceeds \$25,000.00

2.4.10 Contact details

This Policy is administered by the Policy Authority:

State of Arizona
Office of the Secretary of State
1700 W. Washington
Phoenix, Arizona 85007

2.4.10.1 Policy Authority contact person:

Michael Totherow
Phone number: 602.542.6170
E-mail address: pa@mail.sosaz.com

2.4.10.2 Contact person determining CPS suitability for this Policy:

Michael Totherow
Phone number: 602.542.6170
E-mail address: pa@mail.sosaz.com

3 General Provisions

3.1 Obligations

3.1.1 CA obligations

The CA is responsible for all aspects of the issuance and management of a certificate, including control over the application and enrollment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate, and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

The CA will operate in accordance with its CPS, this Certificate Policy, and the laws of Arizona when fulfilling these obligations. The CA will ensure that all LRAs operating on its behalf will comply with the relevant provisions of this CP concerning the operation of LRAs. The CA will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, Certificates or End-Entity hardware and software used within the ESI.

3.1.1.1 *Representations By CA*

By issuing a certificate that references this Policy, the CA certifies to the subscriber, and to all Qualified Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this Policy, that:

- (a) The CA has issued, and will manage, the certificate in accordance with this Policy
- (b) The CA has complied with the requirements of this Policy and its applicable CPS when authenticating the subscriber and issuing the certificate
- (c) There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS
- (d) Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate
- (e) The certificate meets all material requirements of this Policy and the CA's CPS

3.1.1.2 *Time between certificate request and issuance*

There is no stipulation for the period between the receipt of an application for a Certificate and the generation of the Entity's key material.

The CA must ensure that the period for which the Entity has to complete its initialization process is no longer than five working days.

3.1.2 Registration Authorities (RA) and Certificate Manufacturing Authorities (CMA) Obligations

The CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, the CA may delegate

performance of these obligations to an identified Registration Authority (RA) and/or Certificate Manufacturing Authority (CMA) provided that the CA remains primarily responsible for the performance of those services by such third parties in a manner consistent with the requirements of this Policy.

3.1.3 Repository Obligations

The topCA shall be responsible for providing any global certificate and CRL repository that includes all state employees and agents. The PA has discretion to relax this responsibility if it is not realistic. However, the PA retains the authority to require the topCA to fully meet this responsibility at a later time. This repository should be in the form of one or more directories that comply with the State of Arizona's X.500 related standards.

A CA shall be responsible for ensuring that there is at least one certificate and CRL repository associated with it in addition to that of the topCA. The CA may delegate performance of this obligation to an identified Repository Services Provider (RSP), provided that the CA remains primarily responsible for performance of those services by such third party in a manner consistent with the requirements of this Policy. The CA shall use repositories that meet or exceed the State of Arizona's X.500 related standards. The PA retains the right to require the CA to additionally support the global certificate and CRL repository maintained by the topCA.

3.1.4 LRA obligations (LRA duties)

Should the PA allow a CA to use LRAs, then the CA must ensure that all its LRAs comply with all the relevant provisions of this CP and the CA's CPS. The CA shall continue to be responsible for any matters delegated to an LRA.

A CA is responsible through its LRA personnel to bring to the attention of Subscribers all relevant information pertaining to the rights and obligations of the CA, LRA and Subscriber contained in this CP, the Subscriber agreement, if applicable, and any other relevant document outlining the terms and conditions of use.

LRA Administrators must be individually accountable for actions performed on behalf of the CA. (There must be evidence that attributes an action to the person performing the action for it to be individually accountable.) Records of all actions carried out in performance of LRA duties must identify the individual who performed the particular duty.

The LRA is not required to notify a Relying Party of the issuance or revocation of a certificate.

3.1.5 Subscriber Obligations

In all cases, the CA shall require the Subscriber to enter into an enforceable contractual commitment for the benefit of Qualified Relying Parties obligating the Subscriber to:

- (a) activate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key
- (b) acknowledge that by accepting the Certificate the Subscriber is warranting that all information and representations made by the Subscriber that are included in the Certificate are true
- (c) use the Certificate exclusively for authorized and legal purposes, consistent with this Policy

- (d) request the CA to revoke the Certificate promptly upon any actual or suspected compromise of the Subscribers private key

3.1.6 Relying Party Obligations

A Qualified Relying Party has a right to rely on a Certificate that references this Policy only if the Certificate was used and relied upon for lawful purposes and under circumstances where:

- (a) the reliance was reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of reliance
 - (b) the purpose for which the Certificate was used was appropriate under this Policy
 - (c) the Relying Party checked the status of the Certificate prior to reliance and it was valid.
- Reliance in the case of an inability to check the status shall be governed by any contract between the parties and by applicable statute.

3.1.7 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy and its administration.

3.2 Requirements

An issuing CA will ensure that its practices and actions (including certification and repository services, issuance and revocation of certificates, and issuance of CRLs) are in accordance with this CP. It will take reasonable efforts to ensure that all LRAs and Subscribers will know and follow the requirements of this policy when dealing with any certificates containing this policy's OID or the associated keys.

3.2.1 Financial Responsibility

An issuing CA shall meet the greater of the responsibilities outlined here or those established in another CP the issuing CA is approved for, that is, the CA is to meet the greater *set* of responsibilities not the *sum* of the responsibilities.

3.2.1.1 Surety Bond

An issuing Certification Authority shall obtain a bond issued by a surety company authorized to do business in Arizona. Copies of the bond shall be filed with the Treasurer and with the Secretary of State. The amount of the bond shall not be less than twenty-five thousand dollars (\$25,000 US). The bond shall be in favor of the State of Arizona. The bond shall be payable for any penalties assessed by the Secretary of State acting as the Policy Authority pursuant to any losses the State encounters resulting from a Certification Authority's conduct subject to the Electronic Signature Act or arising out of a violation of the Electronic Signature Act or any Rule promulgated thereunder.

This bond shall also be part of any assessment of charges for the transfer and continuation of services (e.g. Repositories) should the Certification Authority or any agent be unable to continue providing any service as required by this Certificate Policy or any related agreement.

Agencies contracting with for-profit Certificate Authorities may incorporate additional bonding requirements in any contract for services with a Certification Authority.

3.2.1.2 Insurance

An issuing Certification Authority shall obtain indemnity insurance coverage (e.g. "errors and omissions," "cyber coverage" or similar coverage) to protect subscribers, relying parties and the State for any losses resulting from the Certification Authority's conduct of activities subject to the Electronic Signature Act or arising out of a violation of the Electronic Signature Act, any Rule promulgated thereunder or any contractual agreement between the issuing CA and the Policy Authority or other agent of the state of Arizona. Indemnity coverage shall be obtained and maintained in the amount of not less than one hundred thousand dollars (\$100,000 US) per occurrence and not less than one million dollars (\$1,000,000 US) for all occurrences. Certificates of insurance acceptable to the State of Arizona shall be issued and delivered prior to Certification Authority approval and the certificates shall identify this CP and include certified copies of endorsements along with a provision that coverages afforded will not be canceled without 60 days prior written notice to the Policy Authority.

This insurance shall also cover any assessment of charges for the transfer and continuation of services (e.g. Repositories) not covered by the surety bond should the Certification Authority or any agent be unable to continue providing any service as required by this Certificate Policy or any related agreement. All coverages, conditions, limits and endorsements shall remain in full force and effect as required to act as an approved Certification Authority.

An issuing Certification Authority shall provide annual evidence of having this insurance in full force and effect.

Agencies contracting with for-profit Certificate Authorities may incorporate additional insurance requirements in any contract for services with a Certification Authority.

3.2.1.3 Consequences of failure to meet Financial Responsibilities

The failure of a Certification Authority to continuously maintain this surety bond and indemnity insurance coverage shall constitute a material breach of contract upon which the State may immediately suspend or terminate approval to issue certificates and may also be the basis for revocation or suspension of the Certification Authority's approval to conduct activities for certificates previously issued under this CP.

Any decision by the State to not take such steps in full and immediate measure in the event of a breach of contract does not preclude the State taking such steps later in the case of the same breach of contract or in the case of a later breach of contract.

3.3 Disclaimers of warranties and obligations

The State of Arizona assumes no liability whatsoever in relation to the use of AESI Certificates or associated public/private key pairs for any use other than in accordance with this CP and any other explicit agreements.

The State of Arizona, its employees and agents makes no representations, warranties or conditions, express or implied other than as expressly stated in this CP or in any other official document.

3.4 Liability

A CA is responsible to Qualified Relying Parties for direct damages suffered by such Relying Parties that are caused by the failure of the CA to comply with the terms of this Policy, and

sustained by such Relying Parties as a result of reliance on a Certificate in accordance with this Policy, but only to the extent that the damages result from the use of Certificates for a suitable applications listed as defined in this CP.

Except as expressly provided in this Policy and in its CPS, CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

3.5 Interpretation & Enforcement

3.5.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the laws of the State of Arizona and the United States of America.

3.5.2 Severability, survival, merger, notice

Any CA, or agent of a CA, shall ensure that any of its agreements will have appropriate provisions governing severability, survival, merger or notice.

Any CA or agent of a CA shall have PA approval of its provisions governing severability, survival, merger or notice before beginning operation within AESI and shall gain approval of any amendment to those provisions before such amendment can take effect.

3.5.3 Dispute Resolution Procedures

Each CA shall ensure that any agreement it enters into provides appropriate dispute resolution procedures.

3.6 Fees

CA shall not impose any fees on the reading of this Policy or its CPS.

CA may charge the Subscriber access fees on Certificates, Certificate status information, or CRLs, subject to agreement between the CA and Subscriber and in accordance with a fee schedule published by the CA in its CPS or otherwise publicly available.

3.7 Publication & Repositories

3.7.1 Publication Of CA Information

Each Approved CA shall cause the operation of a secure on-line Repository that is available to Qualified Relying Parties and that contains (1) issued Certificates that reference this Policy, (2) a Certificate Revocation List ("CRL") or on-line certificate status database, (3) the CA's Certificate for its signing key, (4) past and current versions of the CA's CPS, (5) a copy of this Policy, and (6) other relevant information relating to Certificates that reference this Policy.

3.7.2 Frequency of Publication

All information to be published in the Repository shall be published promptly after such information is available to the CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such Certificate by the Subscriber.

3.7.3 Access Controls

The Repository will be available to Qualified Relying Parties on a basis that is stipulated by the Policy Authority when approving the CA for this CP and the CA's then current terms of access under the corresponding CPS. CA shall not impose any access controls on this Policy, the CA's certificate for its signing key, and past and current versions of the CA's CPS. CA may impose access controls on Certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and Subscriber, in accordance with provisions published in its CPS or otherwise.

3.8 Compliance Audit

The Policy Authority shall outline specific requirements for a compliance audit. These requirements will conform to any statutory or regulatory requirements of the State of Arizona.

Before initial approval as an Approved CA, and thereafter deemed necessary by the PA, the CA (and each RA, CMA, and RSP, as applicable) shall submit to a compliance audit by an independent nationally recognized security audit firm that is approved by the Policy Authority as being qualified to perform such an audit and that has significant experience in the application of PKI and cryptographic technologies. The purpose of such audit shall be to verify that the CA and its delegated parties have a system in place:

- to assure the quality of the CA services provided,
- that the CA complies with all of the requirements of this Policy and its CPS, and
- that assures the CA's CPS is consistent with the requirements of this Policy and any related agreement with the PA.

3.9 Confidentiality Policy

Information regarding subscribers that is submitted on applications for Certificates will be kept confidential by the CA and shall not be released without the prior consent of the Subscriber, unless otherwise required by law. This does not apply, however, to information appearing on certificates.

3.10 Intellectual property rights

No stipulation.

4 Identification And Authentication

4.1 Initial Registration

Subject to the requirements noted below, Certificate applications may be communicated from the applicant to the CA or an RA, (and authorizations to issue certificates may be communicated from an RA to the CA),

- electronically via E-mail or a web site, provided that all communication is secure, such as by using SSL or a similar security protocol,

- by first class U.S. mail, or
- in person.

4.1.1 Types of Names

The subject name used for certificate applicants shall be a unique X.509 Distinguished Name (DN).

4.1.2 Name Meanings

The subject name listed in a Certificate must have a reasonable association with the authenticated name of the Subscriber. In the case of individuals this should be a combination of first name and/or initials and surname. In the case of an organization the name should reflect the legal name of the organization and/or unit.

A Certificate that refers to a role or position shall also contain the identity of the person who holds that role or position.

Any Certificate issued for a device or application shall, within the DN, include the name of the person or organization responsible for that device or application.

4.1.3 Rules For Interpreting Various Name Forms

No stipulation.

4.1.4 Name Uniqueness

The subject name listed in a Certificate shall be unambiguous and unique for all certificates issued by the CA. and conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the CA.

No wildcard name forms are allowed. Each name shall be unique and for a single unique entity.

4.1.5 Verification of Key Pair

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol.

4.1.6 Authentication of Organization

When a CA receives a certificate application from an organization, it shall conduct an independent investigation in order to determine whether:

- The organization legally exists and conducts business at the address listed in the certificate application.
- An Affiliated Individual who is a duly authorized representative of the organization named therein signs the certificate application.
- The information contained in the certificate application is correct.

In conducting its review and investigation, the CA shall review official government records and/or engage the services of a reputable third party vendor of business information to provide validation information concerning each organization applying for a certificate, including legal company name, type of entity, year of formation, names of directors and officers, address, telephone number, and good standing in the jurisdiction where the applicant is incorporated or otherwise organized.

The CA will keep a record of the type and details used for verifying identity.

The Affiliated Individual who signed the certificate application, or their authenticated designee, will be issued a Medium or High certificate in a manner consistent with this CP and CP addendum. All Affiliated Individual certificates issued thereafter will be authenticated in a manner consistent with this CP and CP and within an authorization chain connecting to this initial authenticated affiliate of the organization.

4.1.7 Authentication of Individual -- No Affiliation

4.1.7.1 Identification

In authenticating an unaffiliated individual applicant, the CA or RA shall require proof of identity as defined in the following section *Satisfactory Evidence of Identity*.

Copies of the identification used to establish the subscriber's identity shall be initialed by the CA or RA upon acceptance and archived.

4.1.7.2 Investigation And Confirmation

No Stipulation

4.1.7.3 Personal Presence

Authentication of an unaffiliated individual requires that the applicant must either (1) personally present himself or herself to a CA or RA to be authenticated prior to certificate issuance, or (2) securely deliver signed and notarized copies of the requisite identification to the CA or the RA (in which case, electronic procedures may be used thereafter). Where the applicant delivers notarized copies of identification to the CA or RA, authentication of such identification will be confirmed through the use of a shared secret (such as a PIN number) that is separately communicated in a trustworthy manner to the applicant and included with the documents delivered as part of the certificate application process.

4.1.8 Authentication of Individual – Affiliated Certificate

4.1.8.1 Identification

The CA may establish a trustworthy procedure whereby a sponsoring organization that has been authenticated by the CA and issued a certificate may designate one or more Responsible Individuals, and authorize them to represent the sponsoring organization in connection with the issuance and revocation of certificates for affiliated individuals. The CA may rely on a designated Responsible Individual appointed by the sponsor to properly authenticate the individual applicant (provided that the CA has previously authenticated the sponsor as an organization and the Responsible Individual as an unaffiliated individual, in accordance with this Policy). The Responsible Party shall require proof of identity as defined in the following section *Satisfactory Evidence of Identity*.

In the absence of the foregoing procedure, affiliated individuals shall be authenticated in the same manner as unaffiliated individuals.

4.1.8.2 Authentication Confirmation Procedure

Authentication of the individual may be confirmed through the use of a shared secret (e.g. a PIN number) that is distributed to the applicant by a trustworthy communication method not used for digital signatures. The shared secret may be distributed directly or through the sponsor as part of the certificate enrollment process.

4.1.8.3 Personal Presence

Applicants that are affiliated with an Approved sponsor can be authenticated through an electronically submitted application, based on an appropriate agreement with the sponsor, the approval of a designated Responsible Individual, and the distribution of PIN numbers or a similar security device.

4.1.8.4 Duties of Responsible Individuals

The Responsible Individual represents the sponsoring organization with respect to the issuance and management of certificates. In that capacity he or she is responsible for properly indicating which subscribers are to receive Certificates.

4.1.9 Authentication of devices or applications

An application for a device or application to be an End-Entity may be made by an approved Subscriber for whom the device's or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant must follow this Policy's requirements as if the Subscriber was applying for the Certificate on its own behalf.

The device Certificate will be revoked if the Subscriber's Certificate is revoked. This type of certificate can only be issued by a CA that can assure accomplishment of such revocation.

4.2 Renewal Applications (Routine Rekey)

Within three months prior to the scheduled expiration of the operational period of a Certificate issued following authentication under this Policy, a Subscriber may request issuance of a new Certificate for a new key pair from the CA that issued the original Certificate, provided the original Certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message based on the old key pair in the original Certificate.

Renewal of an affiliated individual shall require verification that the affiliation still exists. Such verification of affiliation shall be the same as what is required for a new application.

4.3 Rekey After Revocation

Revoked or expired Certificates shall not be renewed. Applicants without a valid Certificate from the CA that references this Policy shall be re-authenticated by the CA or RA on certificate application, just as with a first-time application.

4.4 Satisfactory Evidence of Identity

Each signing community will need to evaluate the levels of risk associated with their signing processes and associate those risks to a framework that defines three levels of trust in evaluating authenticity, reliability, and integrity of signed electronic records. Each of these trust levels should be tied to the potential risk involved in and levels of security for the highest risk type of transaction. The trust levels defined are as follows:

- **Basic** - This level provides a basic level of assurance relevant to transactions where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
- **Medium** - This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
- **High** - This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

This policy will identify appropriate implementations for basic, medium, and high trust levels as far as how the:

- Signer is identified.
- Signer is linked to the signature.
- Signature is linked to the integrity of the record.

4.4.1 Signer Identification

Signer identification refers to the method by which an individual is identified and authorized to use a particular electronic signature method. Signer identification is independent of the signature or records creation technology being employed. However, it is critical to the level of trust that can be attributed to a signed record because the more robust or stringent the method of identification and authorization the more assurance that the signature has been authorized for use by the person who he or she purports to be. The identification and authentication methods for each level of trust are displayed in the table below.⁴

Basic	<ul style="list-style-type: none">• A government entity, its agent or an appropriate individual licensed by a government entity (e.g., notary) as being authorized to confirm identities has for the purposes of issuing or authorizing an electronic signature compared the identity of the individual with two pieces of identification (copies or originals). At least one of these must be a government issued identification containing a photograph (e.g., driver's license, non-driver
-------	---

⁴ The Policy Authority reserves the right to establish a higher standard for any particular signing process than is established here.

	<p>identification, passport); or</p> <ul style="list-style-type: none"> • A sponsoring government entity or its agent has compared trusted information in a data base with user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person; or • By attestation of a supervisor, or administrative or information security officer, or an individual certified or licensed by a government entity as being authorized to confirm identities (e.g., notary) who uses a stamp, seal or other mechanism to authenticate their identity confirmation.
Medium	<ul style="list-style-type: none"> • A government entity, its agent or an appropriate individual certified or licensed by a government entity (e.g., notary) as being authorized to confirm identities has for the purposes of issuing or authorizing compared the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • A sponsoring government entity or its agent has previously established the identity of an individual using a process that satisfies the above requirements and there have been no changes in the information presented.
High	<ul style="list-style-type: none"> • A government entity, its agent, or an appropriate individual certified or licensed by a government entity (e.g., notary) as being authorized to confirm identities, in the presence of the individual for the purposes of authorizing or issuing a signature, compares the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government identification containing a photograph (e.g., driver's license, non-driver identification, passport).

Along with the above identification requirements, the originating government entity or its agent must keep a record of the type and details of identification used and on request make it available to the state entity receiving the signed record for that signed record to be accepted at the purported trust level.

4.4.2 Signer Linkage to Signature

Signer linkage to signature refers to the policy, process and procedures establishing a link between the signer and the information and method used to sign. This linkage has two dimensions.

1. The first dimension is the way by which the unique signature characteristics are linked to the signer. This linkage can be achieved through one thing or by a combination of things only the individual:
 - **Knows** (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key);

- *Possesses* (a token -- e.g., an ATM card or a smart card); or
 - *Is* (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, retinal scan or a fingerprint).
2. The second dimension is trust level. Trust level is closely related to the specific signing method (e.g., shared secrets, biometric, cryptographic keys).

The level of trust of an electronically signed record is in part a function of how convinced the receiving government is that the information used to sign has remained in the sole possession of the individual authorized to use it. In developing the levels of trust for this component of the policy it is assumed that there will be multiple ways to meet the requirements of each level and that multiple methods could theoretically meet the requirements of the same level.

The methods for linking signers to signing information or electronic signatures for each level of trust are displayed in the table below.⁵

Basic	<ul style="list-style-type: none"> • Two shared secrets (e.g., pin, password) where a governmental body has assigned at least one secret and the signer has been provided with and has conformed to appropriate security standards as far as protecting the shared secrets. • A shared secret and a private cryptographic key or biometric information in which the cryptographic key cannot be accessed without the shared secret. "Private" in this sense means in the sole possession of the signer.
Medium	<ul style="list-style-type: none"> • Three shared secrets in which one has been assigned by a governmental body and one consists of private information that only the signer would know (e.g., income tax information), and the third could be selected by the signer. • A shared secret and a private cryptographic key or biometric stored in a secure software token on a secure computer.
High	<ul style="list-style-type: none"> • A shared secret and a cryptographic key or biometric stored on a hardware token where the key or biometric cannot be accessed without the shared secret and the shared secret is only known by the signed and the hardware token. • A biometric where the signer needs to be present to sign.

Along with the above identification requirements, the originating government entity or its agent must keep a record of the methods and approaches used to link a signer to signature information.

4.4.3 Signature Linkage to the Integrity of the Record

This element of trust has two components.

⁵ The Policy Authority reserves the right to establish a higher standard for any particular signing process than is established here.

1. An electronic signature must be linked to the record to which it is affixed or associated. E-signatures can be linked to an e-record in many different ways. The e-signature can become part of the record's data structure or imbedded as a data object within the document. The e-signature can also be stored in a different location but logically linked to the e-record. However, a government agency must manage the e-record and electronic signature as a unit and ensure that the link between them is maintained for the record's legal minimum retention period.
2. There must be some method to ensure that the signature is linked to the record content that the signer intended to sign in such a manner that any change to the record since the record was signed is detectable and invalidates the signature.

This signature linkage to the integrity of the record can be achieved by the system that collectively manages the e-record and the associated signature. In such a case, trust is a function of the system's trustworthiness and its controls to ensure that a record or signature has not been tampered with or modified and the system's ability to detect that such has occurred. However, transferring agencies also need to use a transmission method to ensure that the integrity of the electronically signed record is not compromised. Linkage can also be created using technologies in which the signature and record exist as a unified object in which validation of the signature itself provides assurances that the record and signature have not been tampered with or modified. Technologies that use cryptography and hashing techniques can achieve this outcome.

The methods for linking an electronic signature to the integrity of the record for each level of trust are displayed in the table below.⁶

Basic	<ul style="list-style-type: none"> • Self-certification that the system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link.⁷ Transferring agencies have mutually agreed to a secure method for: transferring the electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link.
Medium	<ul style="list-style-type: none"> • An outside entity or auditor has certified that the system used to capture and manage the electronically signed record reasonably ensures, through compliance with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to: a secure method for transferring the electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link. • Self-certification that system used to capture and manage the

⁶ The Policy Authority reserves the right to establish a higher standard for any particular signing process than is established here.

⁷ NIST SP 800-14*Generally Accepted Principles and Practices for Securing Information Technology Systems* will serve as a general guideline for generally accepted system security practices.

	electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to secure methods for ascertaining the integrity of the record and the integrity of the signature and record link. Transferring agencies use a secure network or secure cryptographic method (e.g., secure socket layer (SSL) or VPN to transfer the electronic signed record.
High	<ul style="list-style-type: none"> An outside entity or auditor has certified that the system used to capture and manage electronically signed record reasonably ensures, through compliance with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to: a secure method for transferring the electronically signed record and secure methods for ascertaining the integrity of the record and the integrity of the signature and record link. Transferring agencies use a secure network or secure cryptographic methods (e.g., secure socket layer (SSL) or VPN to transfer the electronic signed record. Self-certification that the system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to a secure method for transferring the electronically signed record and to the use of a cryptographic method with hashing techniques to ensure record integrity and the link between the record and the signature (e.g., PKI).

The ESI electronic signature level (Basic, Medium, High) is determined from this matrix of trust levels. The Certificate assigned should support the highest trust level required among the categories: Signer Identification, Signer Linkage to Signature, Signature Linkage to the Integrity of the Record. The Policy Authority reserves the right to establish a higher standard for any particular signing process than is established here.

5 Operational Requirements

5.1 Certificate Application

An applicant for a Certificate shall complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the CA. All applications are subject to review, approval and acceptance by CA. The certificate application process may be initiated by the following persons:

Potential Subscriber

Individual (unaffiliated)
Individual affiliated with a sponsor

Organization

Authorized Initiator

Potential subscriber only
Potential subscriber or duly authorized representative of sponsor
Duly authorized representative of the

subscribing organization
(who shall be individually
responsible for the certificate.)

5.1.1 Application for a cross-certificate

The PA will identify the necessary procedures to apply for a cross-certificate.

An application for a cross-certificate does not oblige the PA to authorize a cross-certificate. The PA shall review any CA's request for cross-certification and approve or deny any such request according to established procedures.

A CA requesting cross-certification through the topCA will include with the application:

- its Certificate Policy;
- an external audit inspection report validating the assurance level stated in the CP;
- the public verification key generated by the CA.

5.2 Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with this Policy, and complete and final approval of the certificate application, the CA shall issue the requested Certificate, notify the applicant thereof, and make the Certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the Subscriber only. A CA will not issue a Certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

5.3 Certificate Acceptance

The CA shall contractually require that the Subscriber expressly indicate acceptance or rejection of the Certificate following its issuance, in accordance with procedures established by the CA and specified in the CPS.

There will be a short time period when the Subscriber must act to accept, once the time has expired, the Certificate will be revoked and the Subscriber will have to begin a new application.

5.4 Certificate Revocation

5.4.1 Circumstances For Revocation

5.4.1.1 Permissive Revocation

A Subscriber may request revocation of their individual Certificate at any time for any reason.

A sponsoring organization may, where applicable, request revocation of an affiliated individual Certificate at any time for any reason.

The issuing CA may also revoke a Certificate upon failure of the Subscriber (or any sponsoring organization, where applicable) to meet its obligations under this Certificate Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the

Certificate that may be in force. This includes revoking a Certificate when a suspected or known compromise of the private key has occurred.

The PA may, at its discretion, revoke a cross-certificate when a CA fails to comply with obligations set out in this CP, any agreement or any applicable law.

5.4.1.2 Required Revocation

A Subscriber, or a sponsoring organization (where applicable) shall promptly request revocation of a Certificate:

- whenever any of the information on the Certificate changes or becomes obsolete
- whenever the private key, or the media holding the private key, associated with the certificate is known or suspected of being compromised
- whenever an affiliated individual is no longer affiliated with the sponsor

The issuing CA shall revoke a Certificate:

- upon request of the Subscriber or sponsoring organization
- upon failure of the Subscriber (or the sponsoring organization, where applicable) to meet its material obligations under this Certificate Policy, any applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.
- if knowledge or reasonable suspicion of compromise is obtained
- if the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS

Where a CA is cross-certified with the topCA, the topCA must revoke a cross-certificate:

- when any of the information in the Certificate changes;
- upon suspected or known compromise of the private key;
- upon suspected or known compromise of the media holding the private key.

In the event that the CA ceases operations, all Certificates issued by the CA shall be revoked prior to the date that the CA ceases operations.

5.4.2 Procedure For Revocation Request

A certificate revocation request should be promptly communicated to the issuing CA, either directly or through an RA. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber, or the sponsoring organization (where applicable). Alternatively the Subscriber, or sponsoring organization (where applicable), may request revocation by contacting the CA or an authorized RA in person and providing adequate proof of identification in accordance with this Policy.

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the old key pair. The identity of a person submitting a revocation request in any other manner shall be authenticated. Revocation requests authenticated on the basis of the old (compromised) key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke Certificates.

Requests for revocation of Certificates will be logged.

5.4.2.1 Repository/CRL Update

Promptly following revocation of a Certificate, the CRL or certificate status database in the Repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CA shall be archived.

Promptly following revocation of a cross-certificate, the revocation will be published in the ARL of the Issuing CA.

5.4.3 Revocation Request Grace Period

Requests for revocation shall be processed within twenty four hours of receipt by the CA.

5.4.4 Certificate Suspension

Certificate suspension is not allowed.

5.4.5 CRL Issuance Frequency

When CRLs are used, an up-to-date CRL shall be issued at least every three hours.

The updated CRL must be issued immediately when a Certificate is revoked due to key compromise.

The CA will synchronize any CRL issuance with any State directory services that relies on the CA's certificates to determine access to State resources.

5.4.6 CRL checking requirements

A Relying Party must check the status of all certificates in the certificate validation chain against the current CRLs and ARLs prior to their use. A Relying Party must also verify the authenticity and integrity of CRLs and ARLs.

5.4.7 On-Line Revocation/Status Checking Availability

Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated and checked according to the same requirements as defined for a CRL.

5.4.8 Special requirements rekey compromise

A CA must immediately notify all CAs to whom it has issued cross-certificates and the PA after the compromise or suspected compromise of its signing key.

Any other Entity must notify the issuing CA immediately in the event of the compromise or suspected compromise of its signing key.

A CA must ensure that provisions outlining the means it will use to provide notice of compromise or suspected compromise are in its CPS or a publicly available document and appropriate agreements.

5.5 Computer Security Audit Procedures

All significant security events on the CA system should be automatically recorded in audit trail files. The audit log shall be processed at least once a week. Such files shall be retained for at least six (6) months onsite, and thereafter shall be securely archived according to the PA's record retention schedule.

5.6 Records Archival

5.6.1 Types Of Records Archived

The following data and files must be archived by or on behalf of the CA:

- All computer security audit data
- All certificate application data
- All certificates, and all CRLs or certificate status records generated
- Key histories
- All correspondence between the CA and RAs, CMAs, RSPs, and/or subscribers.

The CA is responsible for the satisfactory archiving of this material.

5.6.2 Retention Period For Archive

Archive of the key and certificate information must be retained for at least 30 years. Archives of the audit trail log files must be retained for at least six (6) months.

Any signed document may also have public records retention requirements that must also be met.

5.6.3 Protection Of Archive

The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. This protection must meet or exceed State of Arizona and Agency electronic records retention requirements for such material.

5.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

5.6.5 Archive Collection System (Internal Or External)

No stipulation.

5.6.6 Procedures To Obtain And Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives.

5.7 Key Changover

No stipulation.

5.8 Compromise And Disaster Recovery

5.8.1 Disaster Recovery Plan

The CA must have in place an appropriate disaster recovery and business resumption plan. The plan must set up and render operational a facility located in a geographic diverse area that is capable of providing CA Services in accordance with this Policy within forty eight (48) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be referenced within the CPS or other appropriate documentation and readily available to Qualified Relying Parties for inspection.

5.8.2 Key Compromise Plan

The CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue Certificates, or used by any higher level CA. Such plan shall include procedures for revoking all affected Certificates and promptly notifying all Subscribers and all Qualified Relying Parties.

5.9 CA Termination

In the event that the CA ceases operation, all Subscribers, sponsoring organizations, RAs, CMAs, RSPs, and Qualified Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination. All current and archived CA identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to the PA (or designate) within 24 hours of CA cessation and in accordance with this Policy. Transferred data shall not include any non-AESI data. No key recovery enabled repository data will be comingled with this data.

6 Physical, Procedural And Personnel Security

6.1 Physical Controls

6.1.1 Physical Security -- Access Controls

The CA, and all RAs, CMAs and RSPs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section on Procedural Controls (6.3.1). Access shall be controlled through the use of: electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

6.2 Procedural Controls

6.2.1 Trusted Roles

All employees, contractors, and consultants of CA (collectively "personnel") that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

6.2.2 Multiple Roles (Number Of Persons Required Per Task)

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a CA server should be shared by multiple roles and individuals. Each account on the CA server shall have limited capabilities commensurate with the role of the account holder.

6.3 Personal Security Controls

6.3.1 Background And Qualifications

CAs, RAs, CMAs, and RSPs shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

6.3.2 Background Investigation

CAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

6.3.3 Training Requirements

All CA, RA, CMA, and RSP personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

6.3.4 Documentation Supplied To Personnel

All CA, RA, CMA, and RSP personnel must receive and read comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

7 Technical Security Controls

7.1 Key Pair Generation And Installation

7.1.1 Key Pair Generation

Key pairs for CAs, CMAs, RAs, RSPs, and subscribers must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Acceptable ways of accomplishing this include:

- Having all users (CAs, CMAs, RAs, RSPs, and subscribers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else
- Having keys generated in hardware tokens from which the private key cannot be extracted.

CA, RA, and CMA keys must be generated in hardware tokens. Key pairs for RSPs, and end-entities can be generated in either hardware or software.

7.1.2 Private Key Delivery To Entity

See Section on Physical Security - Access Controls (6.1.1).

7.1.3 Subscriber Public Key Delivery To CA

The Subscriber's public key must be transferred to the RA or CA in a way that ensures that:

- it has not been changed during transit;
- the sender possesses the private key that corresponds to the transferred public key; and
- the sender of the public key is the legitimate user claimed in the certificate application.

7.1.4 CA Public Key Delivery To Users

The public key of the CA signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX Part 3, or via another appropriate mechanism.

7.1.5 Key Sizes

Minimum key length for other than elliptic curve based algorithms is 1024 bits.

Minimum key length for elliptic curve group algorithms is 170 bits (M.J.Wiener, "Performance Comparison of Public-Key Cryptosystems", RSA CryptoBytes, Volume 4, Number 1, Summer 1998).

Acceptable algorithms for public key cryptography applications include:

RSA (Rivest, Shamir, Adelman)	-- digital signature and information security
ElGamal	-- digital signature and information security
Diffie * Hellman	-- digital signature and information security
DSA /DSS (Digital Signature Algorithm)	-- digital signature applications

7.2 CA Private Key Protection

The CA (and the RA, CMA, and RSP) shall each protect its private key(s) in accordance with the provisions of this Policy.

7.2.1 Standards For Cryptographic Module

No stipulation.

7.2.2 Private Key (N-M) Multi-Person Control

No stipulation.

7.2.3 Private Key Escrow

CA signing private keys shall not be escrowed.

7.2.4 Private Key Backup

An entity may optionally back up its own private key.

7.2.5 Private Key Archival

An entity may optionally archive its own private key.

7.2.6 Private Key Entry Into Cryptographic Module

No stipulation.

7.2.7 Method Of Activating Private Key

No stipulation.

7.2.8 Method Of Deactivating Private Key

No stipulation.

7.2.9 Method Of Destroying Private Key

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed.

7.3 Other Aspects Of Key Pair Management

7.3.1 Public Key Archival

The issuing CA must retain all verification public keys.

7.3.2 Key Replacement

CA key pairs must be replaced at least every two (2) years. RA and subscriber key pairs must be replaced not less than every two (2) years and a new certificate issued

7.3.3 Restrictions On CA's Private Key Use

The CA's signing key used for issuing certificates that conform to this Policy shall be used only for signing certificates and, optionally, CRLs.

A private key used by an RA or RSP for purposes associated with its RA or RSP function shall not be used for any other purpose without the express permission of the CA.

A private key held by a CMA and used for purposes of manufacturing certificates for the CA is considered the CA's signing key, is held by the CMA as a fiduciary for the CA, and shall not be used for any reason without the express permission of the CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

7.4 Activation Data

No stipulation.

7.5 Computer Security Controls

All CA servers must include the following functionality either provided by the operating system, or through a combination of operating system, PKI application, and physical safeguards:

- *access control to CA services and ESI roles;*
- *enforced separation of duties for ESI roles;*
- *identification and authentication of ESI roles and associated identities;*
- *object re-use or separation for CA random access memory;*
- *use of cryptography for session communication and database security;*
- *archival of CA and End-Entity history and audit data;*
- *audit of security related events;*
- *self-test of security related CA services;*
- *trusted path for identification of PKI roles and associated identities;*
- *recovery mechanisms for keys and the CA system.*

8 Certificate And CRL Profiles

8.1 Certificate Profile

Certificates that reference this Policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages -- i.e., public keys used for digital signature verification.

All certificates that reference this Policy will be issued in the X.509 version 3 format and will include a reference to the OID for this Policy within the appropriate field. The CPS shall identify the certificate extensions supported, and the level of support for those extensions.

8.1.1 Certificate extensions

The PKI End-Entity software will support all the base (non-extension) X.509 fields:

- *Version: version of X.509 certificate*
- *Serial Number: unique serial number for certificate*
- *Signature: CA signature to authenticate certificate*
- *Issuer: name of CA*
- *ValidityPeriod: activation and expiration date for certificate*
- *Subject: Subscriber's distinguished name*
- *Subject Public Key Information: algorithm ID, key*

No extension shall modify or undermine the use of these base fields. Additionally,
The certificatePolicies field must be set as critical in all AESI PKI certificates.
Every DN must be in the form of an X.501 printableString.
A CA must include and mark as critical the policyConstraints extension.
Critical extensions shall be interpreted as defined in PKIX.

8.2 CRL Profile

If utilized, CRLs will be issued in the X.509 version 2 format. The CPS shall identify the CRL extensions supported and the level of support for these extensions.

8.2.1 Version number

The CA must issue X.509 CRLs in accordance with the PKIX Certificate and CRL Profile.

8.2.2 CRL and CRL entry extensions

All Entity PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. The CPS must define the use of any extensions supported by the CA, its LRAs and End Entities.

9 Policy Administration

9.1 Policy Change Procedures

9.1.1 List Of Items

Notice of all proposed changes to this Policy under consideration by the Policy Authority that may materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details) will be provided to Approved CAs, and will be posted on the World Wide Web site of the Policy Authority. Approved CAs shall post notice of such proposed changes in their repositories and shall advise their subscribers, in writing or by e-mail, of such proposed changes.

9.1.2 Comment Period

Impacted users may file comments with the Policy Authority within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

9.2 Publication & Notification Procedures

A copy of this Policy is available in electronic form on the Internet at <http://www.sos.state.az.us/pa> and via e-mail from pa@mail.sosaz.com.

Approved CAs shall post copies of this Policy in their repositories.

9.2.1.1 Notification mechanism

The PA will notify, in writing, all CAs that are directly cross-certified with the AESI of any proposed changes to this certificate policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. The PA may request CAs to notify their Subscribers of the proposed changes.

9.2.1.2 Mechanism to handle comments

Written and signed comments on proposed changes must be directed to the PA. Decisions with respect to the proposed changes are at the sole discretion of the PA.

9.2.2 Items whose change requires a new policy

If a policy change is determined by the PA to warrant the issuance of a new policy, the PA may assign a new Object Identifier (OID) for the modified policy.

9.3 CPS approval procedures

A CA's accreditation into the AESI PKI must be in accordance with procedures specified by the PA.

Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available.